



# FortiSwitch Release Notes

Version 6.2.5

## **FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

## **FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

## **FORTINET BLOG**

<https://blog.fortinet.com>

## **CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

## **FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

## **FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

## **FORTIGUARD CENTER**

<http://www.fortiguard.com>

## **FORTICAST**

<http://forticast.fortinet.com>

## **END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

## **FORTINET PRIVACY POLICY**

<https://www.fortinet.com/corporate/about-us/privacy.html>

## **FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



FortiSwitch Release Notes

September 11, 2020

11-625-663133-20200911

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
Supported models	5
What's new in FortiSwitchOS 6.2.5	5
<b>Special notices</b>	<b>6</b>
Supported features for FortiSwitchOS 6.2.5	6
Connecting multiple FSW-R-112D-POE switches	13
<b>Upgrade information</b>	<b>14</b>
Cooperative Security Fabric upgrade	14
<b>Product integration and support</b>	<b>15</b>
FortiSwitch 6.2.5 support	15
<b>Resolved issues</b>	<b>16</b>
<b>Known issues</b>	<b>17</b>

## Change log

Date	Change Description
September 11, 2020	Initial release for FortiSwitchOS 6.2.5

# Introduction

This document provides the following information for FortiSwitch 6.2.5 build: 0219.

**NOTE:** The build number is different for all 4xxE models.

- [Supported models on page 5](#)
- [Special notices on page 6](#)
- [Upgrade information on page 14](#)
- [Product integration and support on page 15](#)
- [Resolved issues on page 16](#)
- [Known issues on page 17](#)

See the [Fortinet Document Library](#) for FortiSwitch documentation.

## Supported models

FortiSwitch 6.2.5 supports the following models:

<b>FortiSwitch 1xx</b>	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE
<b>FortiSwitch 2xx</b>	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
<b>FortiSwitch 4xx</b>	FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE, FS-448E, FS-448E-POE, FS-448E-FPOE
<b>FortiSwitch 5xx</b>	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
<b>FortiSwitch 1xxx</b>	FS-1024D, FS-1048D, FS-1048E
<b>FortiSwitch 3xxx</b>	FS-3032D, FS-3032E
<b>FortiSwitch Rugged</b>	FSR-112D-POE, FSR-124D

## What's new in FortiSwitchOS 6.2.5

FortiSwitch 6.2.5 is a patch release only. No new features or enhancements have been implemented in this release.

## Special notices

### Supported features for FortiSwitchOS 6.2.5

The following table lists the FortiSwitch features in Release 6.2.5 that are supported on each series of FortiSwitch models. All features are available in Release 6.2.5, unless otherwise stated.

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
<b>Management and Configuration</b>									
CPLD software upgrade support for OS	—	—	—	—	—	—	—	1024D 1048D	—
Firmware image rotation (dual-firmware image support)	—	✓	✓	148E 148E-POE	✓	✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓	✓	✓	✓	✓	✓	✓
Support for switch SNMP OID	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP conflict detection and notification	✓	✓	✓	✓	✓	✓	✓	✓	✓
FortiSwitch Cloud configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓
<b>Security and Visibility</b>									
802.1x port mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
802.1x enhancements, including MAB	✓	✓	✓	✓	✓	✓	✓	✓	✓
MAB reauthentication disabled	—	✓	✓	✓	✓	✓	✓	✓	✓
open-auth mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
Support of the RADIUS accounting server	Partial	✓	✓	✓	✓	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages	—	✓	✓	✓	✓	✓	✓	✓	✓
EAP Pass-Through	✓	✓	✓	✓	✓	✓	✓	✓	✓
Network device detection	—	—	✓	—	✓	✓	✓	✓	✓
IP-MAC binding	✓	—	—	—	—	—	✓	✓	✓
sFlow	✓	✓	✓	—	✓	✓	✓	✓	✓
Flow export	—	—	✓	—	✓	✓	✓	✓	✓
ACL	—	—	✓	—	✓	✓	✓	✓	✓
Multistage ACL	—	—	—	—	—	—	✓	✓	✓
Multiple ingress ACLs	—	—	✓	—	✓	✓	✓	✓	✓
Schedule for ACLs	—	—	✓	—	✓	✓	✓	✓	✓
DHCP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓
Allowed DHCP server list	—	✓	✓	✓	✓	✓	✓	✓	✓
DHCP blocking	—	—	✓	—	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
IP source guard	—	—	✓	—	✓	✓	—	—	—
Dynamic ARP inspection	✓	—	✓	✓	✓	✓	✓	✓	✓
ARP timeout value	—	✓	✓	✓	✓	✓	✓	✓	✓
Access VLANs	—	✓	✓	✓	✓	✓	✓	✓	✓
VLAN tag by ACL	—	—	✓	—	✓	✓	✓	✓	✓
RMON group 1	—	✓	✓	✓	✓	✓	✓	✓	✓
Reliable syslog (RFC 6587)	—	✓	✓	✓	✓	✓	✓	✓	✓
Packet capture	—	—	✓	—	✓	✓	✓	✓	✓
<b>Layer 2</b>									
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	8	8	8	24/48	24/48	24/64
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓	✓	✓
IPv6 RA guard	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP proxy	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP querier	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP transmit	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED: ELIN support	—	✓	✓	✓	✓	✓	✓	✓	✓



Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
LLPD-MED: PoE negotiation	—	✓	✓	✓	✓	✓	✓	—	—
Per-port max for learned MACs	—	—	✓	✓	✓	✓	✓	—	—
MAC learning limit (See Note 4.)	—	—	✓	✓	✓	✓	✓	—	—
Learning limit violation log (See Note 4.)	—	—	✓	✓	✓	✓	✓	—	—
set mac-violation-timer	—	✓	✓	✓	✓	✓	✓	✓	✓
Sticky MAC	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total MAC entries	—	✓	✓	✓	✓	✓	✓	✓	✓
MSTP instances	—	0-15	0-15	0-15	0-15	0-15	0-32	0-32	0-32
STP root guard	—	✓	✓	✓	✓	✓	✓	✓	✓
STP BPDU guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rapid PVST interoperation	—	✓	✓	✓	✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces	—	✓	✓	✓	✓	✓	✓	✓	✓
Private VLANs	✓	—	✓	—	✓	✓	✓	✓	✓
Multi-stage load balancing	—	—	—	—	—	—	—	✓	✓
Priority-based flow control	—	—	—	—	—	—	✓	✓	✓
Storm control	✓	✓	✓	✓	✓	✓	✓	✓	✓
Per-port storm control	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	✓	—	✓	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Percentage rate control	✓	—	✓	—	✓	✓	✓	✓	✓
VLAN stacking (QinQ)	—	—	✓	—	✓	✓	✓	✓	✓
VLAN mapping	—	—	✓	—	✓	✓	✓	✓	✓
SPAN	✓	✓	✓	✓	✓	✓	✓	✓	✓
RSPAN and ERSPAN	—	RSPAN	✓	—	✓	✓	✓	✓	✓
<b>Layer 3</b>									
Static routing (v4 v6)	✓	—	✓	—	✓	✓	✓	✓	✓
Hardware routing offload (v4 v6)	✓	—	✓	—	✓	✓	✓	✓	✓
Software routing only	✓	✓	—	✓	—	—	—	—	—
OSPF (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
RIP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
VRRP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
BGP (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
IS-IS (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
PIM (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
Hardware-based ECMP	—	—	—	—	—	—	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Static BFD	—	—	✓	✓	✓	✓	✓	✓	✓
uRPF	—	—	—	—	—	—	✓	✓	✓
DHCP relay feature	✓	—	✓	✓	✓	✓	✓	✓	✓
DHCP server	—	—	—	—	✓	4xx only	✓	✓	✓
<b>High Availability</b>									
MCLAG (multichassis link aggregation)	Partial	—	—	—	✓	✓	✓	✓	✓
STP supported in MCLAGs	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping support in MCLAG	✓	—	—	—	✓	✓	✓	✓	✓
<b>Quality of Service</b>									
802.1p support, including priority queuing trunk and WRED	✓	—	✓	—	✓	✓	✓	✓	✓
QoS queue counters	—	—	✓	—	✓	✓	✓	✓	✓
QoS marking	—	—	✓	—	✓	✓	✓	✓	✓
Summary of configured queue mappings	✓	—	✓	✓	✓	✓	✓	✓	✓
Egress priority tagging	—	—	✓	—	✓	✓	✓	✓	✓
<b>Miscellaneous</b>									
PoE-pre-standard detection (See Note 1.)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
PoE modes support: first come, first served or priority based (PoE models)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—
Control of temperature alerts	—	✓	✓	—	✓	✓	✓	✓	✓
Split port (See Note 6.)	Partial	—	—	—	—	—	✓	1048E	✓
TDR (time-domain reflectometer)/cable diagnostics support	✓	—	✓	—	✓	✓	✓	—	—
Auto module max speed detection and notification	✓	—	—	—	—	—	✓	✓	—
Monitor system temperature (threshold configuration and SNMP trap support)	—	✓	✓	—	✓	✓	✓	✓	✓
Cut-through switching	—	—	—	—	—	—	—	✓	✓
Add CLI to show the details of port statistics	—	✓	✓	✓	✓	✓	✓	✓	✓
Configuration of the QSFP low-power mode	—	—	—	—	—	—	✓	1048D 1048E	✓
Energy-efficient Ethernet	—	✓	✓	✓	✓	✓	✓	—	—
PHY Forward Error Correction (see Note 5)	—	—	—	—	—	—	—	1048E	3032E

**Notes**

1. PoE features are applicable only to the model numbers with a POE or FPOE suffix.
2. 24-port LAG is applicable to 524D, 524-FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548-FPOE, and 1048D models.
3. To use the dynamic layer-3 protocols, you must have an advanced features license.
4. The per-VLAN MAC learning limit and per-trunk MAC learning limit are not supported on the 448D/448D-POE/448D-FPOE/248E-POE/248E-FPOE/248D series.
5. Supported only in 100G mode (clause 91).
6. On the 3032E, you can split one port at the full base speed, split one port into four sub-ports of 25 Gbps each (100G QSFP only), or split one port into four sub-ports of 10 Gbps each (40G or 100G QSFP).

## Connecting multiple FSW-R-112D-POE switches

The FSW-R-112D-POE switch does not support interconnectivity to other FSW-R-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

# Upgrade information

FortiSwitch 6.2.5 supports upgrading from FortiSwitch 3.5.0 and later.

## Cooperative Security Fabric upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Framework - Upgrade Guide*
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*

This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

# Product integration and support

## FortiSwitch 6.2.5 support

The following table lists 6.2.5 product integration and support information.

<b>Web browser</b>	<ul style="list-style-type: none"><li>• Mozilla Firefox version 52</li><li>• Google Chrome version 56</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>FortiOS (FortiLink Support)</b>	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

## Resolved issues

The following issues have been fixed in 6.2.5. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
619284	The Zabbix SNMP server is not receiving output from the FortiSwitch unit.
626017	When a new link is added to an MCLAG ring topology, too much traffic is dropped.
629721	HTTP and HTTPS connections from the same client or from the same browser do not work.
633433	An internal server error occurs when logging in as admin with HTTPS.
648046, 649564	The network cannot be accessed because of an STP loop in a closed ring topology.
653907	After FortiSwitch units were replaced, three APC network management cards and a Zebra printer cannot be accessed.
658968	The syslog source IP address is a loopback IP address, but the interface is still sending syslog data.



# Known issues

The following known issues have been identified with 6.2.5. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANS).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	<p>When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.</p> <p><b>Workarounds:</b></p> <ul style="list-style-type: none"><li>—Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN.</li><li>—Temporarily disable dhcp-snooping on vlan, issue the <code>execute interface dhcpclient-renew &lt;interface&gt;</code> command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.</li></ul>
510943	<p>The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values.</p> <p><b>Workaround:</b> When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag &lt;physical port name&gt;</code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p>
520954	When a “FortiLink mode over a layer-3 network” topology has been configured, the FortiGate GUI does not always display the complete network.
542031	For the 5xx switches, the <code>diagnose switch physical-ports led-flash</code> command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.

Bug ID	Description
572052	<p>Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters.</p> <p><b>Workaround:</b> Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.</p>
585550	<p>When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.</p>



**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.